

PTO 2003-781

Japan, Kokai

2-37484

IC CARD

[IC Kado]

Kazuhiko Omichi

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C.

December, 2002

Translated by: Schreiber Translations, Inc.

Country : Japan  
Document No. : 2-37484  
Document type : Kokai  
Language : Japanese  
Inventor : Kazuhiko Omichi  
Applicant : Hitachi Maxell, Ltd.  
IPC : G 06 K 19/073  
B 42 D 15/10  
Application date : July 27, 1988  
Publication date : February 7, 1990  
Foreign Language Title : IC Kado  
English Title : IC CARD

1. Title of the Invention: IC CARD

2. Claims

1. An IC card, characterized by the fact that in an IC card that has a processor, a nonvolatile memory for storing programs of the processor, and a volatile memory which stores data and is not backed up by an internal power source or a memory which can be volatilized and exchanges data with an external device, it is equipped with a detection means that detects a stored information showing the storage of an issue processing program for an issue processing among the information being sent from the above-mentioned external device, a program writing means that stores the information of the above-mentioned issue processing program sent in accordance with the detection of the above-mentioned stored information by the detection means into the above-mentioned volatile memory or the above-mentioned memory which can be volatilized, and a program implementation means that implements an issue processing by starting the above-mentioned issue processing program; and after the issue progressing program is implemented by the above-mentioned program implementation means and the issue processing is finished, the above-mentioned issue processing program is erased.

---

\* Numbers in the margin indicate pagination in the foreign text.

2. The IC card testing system of Claim 1, characterized by the fact that the memory which can volatile data is an EEPROM; and the program implementation means erases the issue processing program after finishing the issue processing.

3. The IC card testing system of Claim 1, characterized by the fact that the memory which can volatilize data is a RAM; and the program implementation means cuts off the power supply from the above-mentioned external device by discharging the IC card from the external device after finishing the issue processing and erases the issue processing program.

### 3. Detailed explanation of the invention

(Industrial application field)

The present invention pertains to an IC card. Specifically, the present invention pertains to an improvement of an IC card that does not leave an issue processing program in the IC card.  
(Prior art)

Credit systems in product transactions, or bank payment/deposit systems for exchanging cashes, or various kinds of exact calculation systems in hospitals or employee restaurants /2 are put into practice as systems using IC cards. In these systems using the IC cards, however in the systems using the IC cards, its illegal use causes a big program.

The IC card is usually built with microprocessor, memory, and interface for exchanging data with external devices. For example, it is mounted in a host computer or an IC card

reader/writer as one of the external devices, and a command group transmitted from the external device is decoded, and in accordance with the operation programs stored in the memory, the access of the memory such as writing, reading, and erasing of data is implemented. The result is sent back as a response to the command to the external storage device, and in this sequence, the data are exchanged with the external device.

In such a conventional IC card, data contents such as password number, other identification information, various kinds of control information for internal and external devices of the IC card, and information showing the positions of the storage areas of various kinds of data and its capacities are written as issue data via an external device by an IC card issuer when the card is issued after manufacturing the IC card. For this reason, it is necessary to store an issue processing program for writing issue data into a prescribed memory area in the IC card.

(Problems to be solved by the invention)

The above-mentioned issue processing program has been written and mounted in advance in a mask ROM in a microcomputer of the conventional IC card. Accordingly, when the IC card is used or operated, the issue progressing program remains in the IC card. As a result, data can be read out or written into the IC card by the issue processing program. Therefore, there is a risk in which the contents (password number, etc.) of the IC card are detected or rewritten by others. From such a viewpoint, the conventional IC card is deficient for its secrecy and

reliability.

Also, since the issue processing program which is not required for using and operating exists in a nonvolatile memory in a microcomputer, the storage area of general operation programs becomes an area other than that, so that its length is also restricted.

The present invention solves the drawbacks of such a prior art, and its purpose is to provide an IC card with excellent secrecy and reliability without leaving an issue processing program.

(Means to solve the problems)

The constitution of the IC card of the present invention for achieving such a purpose is characterized by the fact that in an IC card that has a processor, a nonvolatile memory for storing programs of the processor, and a volatile memory which stores data and is not backed up by an internal power source or a memory which can be volatilized and exchanges data with an external device, it is equipped with a detection means that detects a stored information showing the storage of an issue processing program for an issue processing among the information being sent from the external device, a program writing means that stores the information of the issue processing program sent in accordance with the detection of the stored information by the detection means into the volatile memory or the memory which can be volatilized, and a program implementation means that implements an issue processing by starting the issue processing program; and

after the issue progressing program is implemented by the program implementation means and the issue processing is finished, the issue processing program is erased.

(Operation)

Thus, whether or not the information being transmitted from an external device is an issue processing program of the IC card is detected by the detection means, and if it is detected, the information of the issue processing program is written into the volatile memory or the memory. which can be volatilized. by the issue processing program writing means. Then, after finishing the writing, since the program is implemented by the program implementation means, the IC card can be freely issued by an issuer. At the same time, after the issue processing, if the data for the issue processing program are erased in the memory, which can volatilize the data, by the program implementation means, for instance, and in the volatile memory, when the IC card is discharged from the external device, the issue processing program is erased.

As a result, when the IC card is used or operated, the issue /3 processing program does not exist in the IC card, and the space of the volatile memory or the space of the memory which can volatilize data can be utilized as a work area of the operation programs, so that the IC card that can sufficiently utilize a memory area and has excellent secrecy and reliability can be issued.

(Application example)

Next, an application example of the present invention is explained in detail referring to the figures.

Figure 1 is a block diagram showing the internal constitution of the IC card showing an application example of the present invention. Figure 2 is a flow chart showing an issue processing when the IC card is issued.

In Figure 1, 10 is an IC card that is mounted in an external device such as IC card reader/writer or host computer and exchanges data with the external device, and 9 is its information processing part (microprocessor, MPU). Then, control programs or basic processing programs or operation programs of the MPU 9 are stored in a ROM (including mask ROM, PROM, and EEPROM) 3a installed in an arithmetic processing part 3.

In a normal operation, the MPU 9 implements a prescribed processing in accordance with the operation programs stored in the ROM 3a, data transferred from an external device or readout data or result data are temporarily stored in the RAM 4 as a volatile memory, and the data are exchanged with the external devices such as IC card reader/writer. Also, in this case, there is no internal power source, and power sources of RAM 4, etc., are provided from the external devices. In other words, the RAM 4 is not backed up by an internal power source.

5 is an EEPROM, is accessed by the MPU 9, and has an issue data storage area 5a into which issue data such as password number, various kinds of identification information, and control information required for issuing a card and a storage area 5b



that temporarily stores an issue processing program for storing the issue data in the issue data storage area 5a.

Here, the MPU 9 consists of identification means 2, arithmetic processing part 3, issue processing program writing means 6, issue processing program implementation means 7, and issue processing program erasure means 8 as its functional blocks. Then, part or all of these constituent elements may be realized by circuits as the hardware or may also be realized by implementing the corresponding each processing program stored in the RAM 4, EEPROM 5, or ROM 3a. Furthermore, they may also be realized by the combination of the hardware and the software.

Next, the above-mentioned constitution as the characteristic of the present invention and its operation are mainly explained according to the processing flow of Figure 2.

An input and output device 1 is an interface with an external device, and at step (1) of Figure 2, the input and output device 1 receives a data block transmitted from the external device and transmits it to the identification means 2. In the data block, there is a mode identification information part for identifying the mode (the kind of processing) being processed by itself exists, and at the next step (2), it is identified by the identification means 2.

At step (2), first, the mode identification information in the data block is decoded, or its matching is detected, so that it is decided and identified whether an issue processing or a general operation program is implemented. Also, as a

transmission format of the data block, for example, initial start code, command code or response code, mode identification information, transmission data, and final end code are arranged. In the transmission data block from the external device (for example, IC card reader/writer), the command code such as write and readout is inserted into the second position, and as response from the IC card 2, the response code is inserted into the second position.

On the other hand, if it is discriminated by the above-mentioned identification and decision at step (2) that the mode identification information of the data block being transmitted from the external device is an issue processing, furthermore, at the next step (3), the identification means 2 decides whether or not the IC card 10 has been issued, referring to issue flags stored in the identification means 2 or in a specific storage area of the EEPROM 5. In this decision, when it is decided that the issue has not been finished, the issue processing program writing means 6 is started by the identification means 2. /4

Then, at the next step (4), the issue processing program writing means 6 receives the data existing in the data block transmitted from the external device via the identification means 2 and sequentially writes them into the space part of the storage area 5b allocated as an area for storing the issue processing program of an address space in the EEPROM 5.

If the entire writing of the data block transmitted from the external device is finished, the issue processing block writing

means 6 transfers a control right to the arithmetic processing part 3 and starts the issue processing program implementation means 7 via the arithmetic processing part 3.

The issue progressing program implementation means 7 starts the issue processing program stored in the storage area 5b of the EEPROM 5 at step (5) and enters a wait loop for detecting an issue data writing command. Then, if the issue data are transmitted along with the command from the external device, said means receives it and proceeds from step (5) to step (6). At step (6), the issue data such as password number, various kinds of identification information, and control information transmitted from the external device are written into the storage area 5a of the issue data of the EEPROM 5 according to the issue processing program. Here, all the data required for the next issue processing are written, and if the writing processing is normally finished, the response of the issue end is transmitted to the external device at the next step (7). Also, in this case, as the response, the above-mentioned written data may be read out and transmitted to the external device. In such a processing, the external device after receiving the written data can decide whether or not the issue data are correctly written.

Next, the issue processing implementation means 7 starts the issue processing program erasure means 8 via the arithmetic processing part 3. The issue processing program erasure means 8 erases the issue processing program at step (8), sets an issue flag showing the issue end of the EEPROM 5 at step (9), and

finishes the issue. Then, the means is returned to the initial state of step (1). In this manner, only for the issue processing, the issue processing program is loaded in the IC card 10 from the external device by the decision processing of step (2).

On the other hand, when the external device tests the contents of the written issue data or when it is decided at step (6) that the issue data transmitted from the IC card 10 and the data to be actually written into the IC card 10 are different from the decision in the external device, the external device repeats the issue processing of the IC card in a similar sequence from step (1).

The IC card is issued in this manner. Here, in the decision of the previous step (2), if it is decided that the contents shown in the mode identification information do not correspond to the issue processing program, the flow proceeds to step (3)a, and similarly to the case of the above-mentioned step (3), the identification means 2 decides whether or not the issue is finished, referring to the issue flag.

As a result, if it is decided that the IC card has been issued, the data block transmitted from the external device is transferred to the arithmetic processing part 3. The arithmetic processing part 3 decodes the command part of the data block at of step (4)a and implements the processing for the command. Then, the response information of the result processed at step (5)a is transmitted to the external device, and the flow returns

to the initial state of step (1).

On the other hand, in the decision of the previous step (3)a, if it is decided that the issue has not been finished, the response of a command error is transmitted as an error processing to the external device at step (4)b, and the flow returns to the initial state of step (1).

If such an issue processing is finished, the IC card 10 is then discharged from the external device. If the IC card 10 is discharged from the external device, since the IC card 10 does not have a backup power source, all the data of the RAM 4 are /5  
erased. Accordingly, if the above-mentioned issue processing program is stored in the address space allocated to the RAM 4, the erasure processing of the issue processing program of the previous step (8) can be omitted. In other words, if the issue processing program is stored in the RAM 4, the issue processing program is erased when the IC card 10 is discharged.

In this manner, the issue processing program is erased along with the issue processing end, so that only when the IC card is issued by card issuer, etc., the issue processing program exists in the IC card. Thereby, when the IC card is used or operated, an illegal use of readout, write, etc., of data utilizing the issue processing program remaining in the IC card can be prevented.

Also, in this application example, in case part or all of each constituent element of the identification means 2, arithmetic processing part 3, issue processing program writing

means 6, issue processing program implementation means 7, and issue processing program erasure means 8 are stored as programs in the RAM 4 instead of the EEPROM 5, the programs corresponding to these functions are stored in the RAM 4 according to the processing program of the ROM 3a prior to the above-mentioned processing.

As explained above, in this application example, the RAM is used as a volatile memory, and needless to say, an EEPROM which can be volatilized may also be used. Also, the issue processing program written in the EEPROM may be erased by starting the issue processing program erasure means according to the command from the external device. Also, the issue processing program may be implemented according to the command from the external device apart from its writing.

In this application example, the identification means 2, arithmetic processing part 3, issue processing program writing means 6, issue processing program implementation means 7, and issue processing program erasure means 8 are explained as independent means, however they may also be realized by implementing each corresponding processing program by the arithmetic processing part 3.

Also, in this application example, the mode identification information is put into the data block, and whether or not the issue processing program is stored is identified by the mode identification means. However, it may be simply a means that can detect it from the transmitted information and is not limited to

the mode identification means.

In this application example, the type in which commands and data are inserted into the data block and transmitted is mentioned, however needless to say, the commands and the data may also be independently transmitted.

(Effects of the invention)

As explained above, according to the present invention, whether or not the information being transmitted from an external device is an issue processing program of an IC card is detected by the detection means, and if it is detected, the information of the issue processing program is written into the volatile memory or the memory. which can be volatilized. by the issue processing program writing means. Then, after finishing the writing, since the program is implemented by the program implementation means, the IC card can be freely issued by an issuer. At the same time, after the issue processing, the data for the issue processing program are erased in the memory, which can volatilize the data, by the program implementation means, and in the volatile memory, when the IC card is discharged from the external device, the issue processing program is erased.

As a result, when the IC card is used or operated, the issue processing program does not exist in the IC card, and the space of the volatile memory or the space of the memory which can volatilize data can be utilized as a work area of the operation programs. Therefore, the IC card which can sufficiently utilize the memory area and has excellent secrecy and reliability can be

issued.

#### 4. Brief description of the figures

Figure 1 is a block diagram showing the internal constitution of the IC card which is an application example of the present invention. Figure 2 is a flow chart showing an issue processing when the IC card is issued.

/6

- 1 Input and output device
- 2 Identification means
- 3 Processing device
  - 3a ROM
- 4 RAM
- 5 EEPROM
- 6 Issue processing program writing means
- 7 Issue processing program implementation means
- 8 Issue processing program erasure means
- 9 Information processing part
- 10 IC card



第 1 図

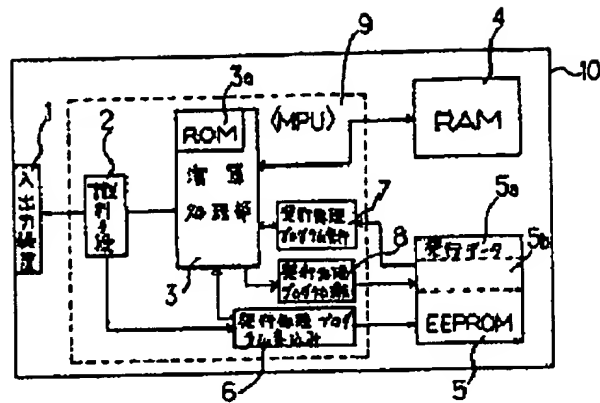


Figure 1:

- 1 Input and output device
- 2 Identification means
- 3 Processing device
- 5a Issue data
- 6 Issue processing program writing means
- 7 Issue processing program implementation means
- 8 Issue processing program erasure means

第 2 図

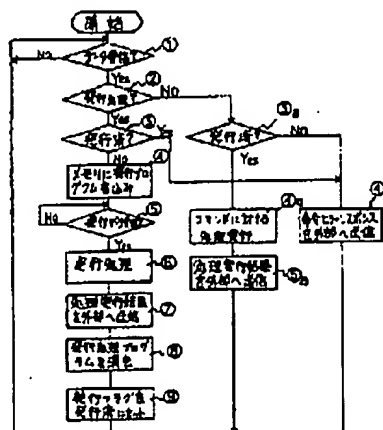


Figure 2:

A. Start

- (1) Data reception ?
- (2) Issue processing ?
- (3) Issue end ?
- (3)a Issue end ?
- (4) Writing of an issue program into a memory
- (4)a Processing implementation for a command
- (4)b Transmission of a command error response to the outside
- (5) Issue data reception ?
- (6) Issue processing
- (7) Transmission of the processing implementation result to the outside
- (8) Erasure o the issue processing program
- (9) Setting an issue flag to the issue end

CLIPPEDIMAGE= JP402037484A

PAT-NO: JP402037484A

DOCUMENT-IDENTIFIER: JP 02037484 A

TITLE: IC CARD

PUBN-DATE: February 7, 1990

INVENTOR-INFORMATION:

NAME

OMICHI, KAZUHIKO

ASSIGNEE-INFORMATION:

NAME

HITACHI MAXELL LTD

COUNTRY

N/A

APPL-NO: JP63187291

APPL-DATE: July 27, 1988

INT-CL (IPC): G06K019/073;B42D015/10

US-CL-CURRENT: 235/487

ABSTRACT:

PURPOSE: To issue an IC card with high confidentiality and reliability by erasing an issued and processed program after the issue processing program is executed with a program executing means, and the issue processing is completed.

CONSTITUTION: Whether or not information transmitted from an external device is for the issue processing program of an IC card 10 is detected, and the information of the issue processing program is written to a volatile memory or a memory 5 which can be made volatile. After the completion of writing, the program is executed by a program executing means 7. Consequently, the IC card 10 can be freely issued corresponding to an issueing person, in the memory 5, the data concerning the issue processing program is erased, and in the volatile

memory 5b, the issue processing program is erased when the IC card is extracted from the external device. Thus, the IC card with high confidentiality and reliability can be issued.

COPYRIGHT: (C)1990,JPO&Japio

## ⑫ 公開特許公報(A) 平2-37484

⑤ Int. Cl.<sup>3</sup>

識別記号

庁内整理番号

⑬ 公開 平成2年(1990)2月7日

G 06 K 19/073  
B 42 D 15/10

5 2 1

6548-2C  
6711-5B

G 06 K 19/00

P

審査請求 未請求 請求項の数 3 (全6頁)

⑭ 発明の名称 ICカード

⑯ 特 願 昭63-187291

⑰ 出 願 昭63(1988)7月27日

⑱ 発 明 者 大 道 和 彦 大阪府茨木市丑寅1丁目1番88号 日立マクセル株式会社  
内

⑲ 出 願 人 日立マクセル株式会社 大阪府茨木市丑寅1丁目1番88号

⑳ 代 理 人 弁理士 梶山 信是 外1名

## 明 細 書

1. 発明の名称 ICカード

2. 特許請求の範囲

(1) プロセッサと、このプロセッサのプログラムを記憶する不揮発性メモリと、データ等を記憶する、内部電源でバックアップされていない揮発性メモリ若しくは揮発させることが可能なメモリとを有し、外部装置との間でデータの授受を行うICカードにおいて、前記外部装置から送出される情報のうちから発行処理のための発行処理プログラムを格納することを示す格納情報を検出する検出手段と、この検出手段が前記格納情報を検出したときにそれに応じて送出された前記発行処理プログラムの情報を前記揮発性メモリ若しくは前記揮発させることが可能なメモリに格納するプログラム書込み手段と、前記発行処理プログラムを起動して発行処理を実行するプログラム実行手段とを備え、前記プログラム実行手段により発行処理プログラムが実行されて発行処理が終了した後に前記発行処理プログラムが消去されることを特徴

とするICカード。

(2) データを揮発させることが可能なメモリはEEPROMであり、プログラム実行手段は、発行処理終了後に発行処理プログラムを消去する処理をすることを特徴とする請求項1記載のICカード。

(3) データを揮発させることが可能なメモリはRAMであり、プログラム実行手段は、発行処理終了後にICカードを外部装置から排出する処理をすることにより前記外部装置からの電力供給を断って発行処理プログラムを消去することを特徴とする請求項1記載のICカード。

3. 発明の詳細な説明

〔産業上の利用分野〕

この発明は、ICカードに関し、詳しくはICカードの内部に発行処理プログラムを残さないで済むようなICカードの改良に関する。

〔従来の技術〕

商品取引でのクレジット方式とか、現金の受け渡しを行う銀行の支払/預金方式、病院とか社員

食堂等における各種の精算方式などがＩＣカードを用いる方式として実用化されているが、このようなＩＣカードによる方式では、その不正使用が大きな問題となる。

ＩＣカードは、通常、内部にマイクロプロセッサとメモリ、そして外部装置との間でデータの授受を行うためのインタフェース等を内蔵していて、例えば、外部装置の１つであるホストコンピュータとか、ＩＣカードリーダー・ライターに装着されて使用され、外部装置から発信されたコマンドをＩＣカードの内部制御プログラムが解釈し、メモリに記憶された動作プログラムに従って、そのメモリをアクセスし、例えばデータの書込み、読出し及び消去等を実行し、その結果をコマンドに対するレスポンスとして外部装置に返答するシーケンスに従って外部装置との間でデータの授受を行う。

従来、このようなＩＣカードでは、そのデータメモリに割当てられる、暗証番号、その他の識別情報、ＩＣカード内部或いは外部装置についての

各種の管理情報、各種データの記憶領域の位置やその容量などを示す情報等のデータ内容については、ＩＣカード製造後のカード発行時に、発行データとしてＩＣカード発行者によって外部装置を介して書込まれる。そのためにＩＣカード側には発行データを所定のメモリ領域に書込む発行処理プログラムを格納しておく必要がある。

#### 〔解決しようとする課題〕

従来、前記の発行処理プログラムは、あらかじめＩＣカードのマイクロコンピュータ内部のマスクＲＯＭに書込まれて実装されている。そこで、ＩＣカードを使用する時とか、その運用時にＩＣカード内部に発行処理プログラムが残されたままとなり、ＩＣカード内部のデータの読出し、書込みがこの発行処理プログラムによって実行可能なものとなる。したがって、ＩＣカードの内容（暗証番号など）が他人に知れてしまったり、書換えられてしまう危険性がある。このような点で、従来のＩＣカードは、その機密性、信頼性に欠けている。

また、使用時、運用時には必要としない発行処理プログラムがマイクロコンピュータ内部の揮発性メモリに存在することから、一般の動作プログラムの格納領域がそれ以外の領域となってしまう、その長さも規制されている。

この発明は、このような従来技術の欠点を解消するものであって、発行処理プログラムを残さないで済み、機密性、信頼性に優れたＩＣカードを発行できるＩＣカードを提供することを目的とする。

#### 〔課題を解決するための手段〕

このような目的を達成するためのこの発明のＩＣカードの構成は、外部装置から送出される情報のうちから発行処理のための発行処理プログラムを格納することを示す格納情報を検出する検出手段と、この検出手段が格納情報を検出したときにそれに応じて送出された発行処理プログラムの情報を揮発性メモリ若しくは揮発させることが可能なメモリに格納するプログラム書込み手段と、発行処理プログラムを起動して発行処理を実行する

プログラム実行手段とを備えていて、プログラム実行手段により発行処理プログラムが実行されて発行処理が終了した後に発行処理プログラムが消去されるものである。

#### 〔作用〕

このように、外部装置から送信される情報に対して検出手段によってＩＣカードの発行処理プログラムについてのものか否かを検出し、それが検出されると、発行処理プログラムの情報が発行処理プログラム書込み手段により揮発性メモリ若しくは揮発させることが可能なメモリ内へ書込まれる。そして、書込み終了後にそのプログラムがプログラム実行手段により実行されるので、発行者対応に自由にＩＣカードの発行処理を行うことができ、かつ発行処理後には、データを揮発させることが可能なメモリでは、発行処理プログラムに関するデータが、例えば、プログラム実行手段により消去され、揮発性メモリでは、ＩＣカードが外部装置から排出されるときに発行処理プログラムが消去される。

その結果、ICカードの使用時或いは運用時には、ICカード内部に発行処理プログラムを残さなくても済み、揮発性メモリの空間若しくはデータを揮発させることが可能なメモリの空間は、動作プログラムのワークエリア等として利用できるようになり、メモリ領域を十分に活用でき、かつ機密性、信頼性に優れたICカードを発行することができる。

#### 〔実施例〕

以下、この発明の一実施例について図面を参照して詳細に説明する。

第1図は、この発明の一実施例を示すICカードの内部構成を示すブロック図、第2図は、ICカード発行時における発行処理のフローチャートである。

第1図において、10は、ICカードリーダー・ライタ又はホストコンピュータ等の外部装置に装着されて、外部装置との間でデータの授受を行うICカードであって、9は、その情報処理部（マイクロプロセッサ、MPU）である。そして、こ

る記憶領域5bとを有している。

MPU9は、その機能ブロックとして、ここでは、識別手段2、演算処理部3、発行処理プログラム書込み手段8、発行処理プログラム実行手段7、そして発行処理プログラム消去手段8とにより構成されている。なお、これら構成要素の一部或いは全部は、ハードウェアとして回路により実現されても、また、RAM4、EEPROM5、或いはROM3aに記憶された対応する各処理プログラムを実行することで実現されてもよい。さらにこれらは、ハードウェアとソフトウェアとの組合せで実現されてもよい。

以下は、この発明の特徴である前記の構成を中心として、その動作について第2図の処理の流れに従って説明する。

入出力装置1は、外部装置とのインタフェースであって、第2図のステップ①において、入出力装置1が外部装置から送信されたデータブロックを受信し、それを識別手段2に送出する。データブロックには、自己が処理するモード（処理の種

のMPU9の制御プログラムとか基本的処理プログラムや動作プログラムがその演算処理部3の内部に設けられたROM（マスクROM、PROM、EEPROMを含む）3aに記憶されている。

通常の動作においては、MPU9がROM3aに記憶された動作プログラムに従って、所定の処理を実行し、揮発性メモリであるRAM4に外部装置から転送されたデータとか、読出しデータ、結果データ等が一時的に記憶され、ICカードリーダー・ライタ等の外部装置との間でデータの授受が行われる。なお、この場合、内部電源はなく、RAM4等の電源は外部装置から供給される。すなわち、RAM4は内部電源でバックアップされていない。

5は、EEPROMであり、MPU9によりアクセスされ、カード発行のために必要な、暗証番号とか、各種の識別情報、そして管理情報等の発行データが格納される発行データ記憶領域5aと、この発行データを発行データ記憶領域5aに記憶するための発行処理プログラムを一時的に記憶す

る識別するモード識別情報部分があって、次のステップ②において、識別手段2によりそれが識別される。

ステップ②では、まず、データブロック中のモード識別情報がデコードされ、又はその一致が検出されることで、発行処理か、一般の動作プログラムを実行するのかの判定がなされてそれが識別される。なお、ここでのデータブロックの伝送フォーマットとしては、例えば、その最初に開始コード、次にコマンドコード又はレスポンスコード、その次にモード識別情報、そして送信データ、最後に終了コード等が配列されるものであって、外部装置（例えば、ICカードリーダー・ライタ）側からの送信データブロックには、第2番目の位置に書込み、読出し等のコマンドコードが挿入され、ICカード2側からの応答では、第2番目にレスポンスコードが挿入される。

さて、前記のステップ②の識別判定によって外部装置側から送出されるデータブロックのモード識別情報が発行処理であると判別されると、さら

に、次のステップ③において、識別手段2は、ICカード10が発行済みのものか否かを、例えば、識別手段2の内部或いはEEPROM5の特定の記憶領域に記憶された発行フラグを参照してそれが立てられているか否かによって判定する。この判定で、発行済みでないと判定されたときには、次に、識別手段2により発行処理プログラム書込み手段8が起動される。

そして、次のステップ④において、発行処理プログラム書込み手段8は、外部装置側から送出されたデータブロックにあるデータを識別手段2を介して受取り、そのデータをEEPROM5内のアドレス空間のうちの発行処理プログラムを格納する領域として割り当てられた記憶領域5bの空間部分へ順次書込んで行く、書込み処理を実行する。

外部装置から送信されたデータブロックの書込みをすべて終了すると、発行処理プログラム書込み手段8は、演算処理部3に制御権を移すとともに、演算処理部3を介して発行処理プログラム実

行手段7を起動する。

発行処理プログラム実行手段7は、ステップ⑤において、EEPROM5の記憶領域5bに記憶された発行処理プログラムを起動し、発行データ書込みコマンドを検出する待ちループに入る。そして、外部装置からこのコマンドとともに発行データが送出されると、これを受信してステップ⑤からステップ⑥へと移り、ステップ⑥において、発行処理プログラムに従って、外部装置から送信された暗証番号、各種の識別情報、管理情報等の発行データをEEPROM5の発行データの記憶領域5aに書込んで行く。ここで次の発行処理に必要なデータをすべて書込み、書込み処理が正常に終了すると、次のステップ⑦において、発行終了の応答を外部装置に送出する。なお、この場合に、応答として前記の書込みデータを読出して外部装置に送信するようにしてもよい。このような処理では、書込まれたデータを受けた外部装置では、発行データ等が正しく書込まれたか否かを判定することができる。

発行処理プログラム実行手段7は、次に演算処理部3を介して発行処理プログラム消去手段8を起動する。発行処理プログラム消去手段8は、ステップ⑧において、発行処理プログラムを消去する処理を行い、ステップ⑨において、EEPROM5の発行済みを示す発行フラグをセットして、発行済みとする。そして、ステップ①の初期状態に戻る。このようにして、ステップ②の判定処理により、発行処理のときにのみ発行処理プログラムを外部装置からICカード10にロードする。

ところで、外部装置が書込み発行データの内容をテストしたとき、或いはステップ⑩においてICカード10側から送られてきた発行データについて外部装置における判定で実際にICカード10に書込むべきデータと送信されたデータとが相違していると判定されたときには、外部装置は、再び、ステップ①から同様な手続きでICカードの発行処理を繰り返す。

このようにしてICカードの発行を行うものであるが、ここで、先のステップ②の判定において、

モード識別情報に示される内容が発行処理プログラムに対するものでないと判定された場合には、ステップ④aへと移行して、ここでも前記ステップ③の場合と同様に識別手段2が発行フラグを参照して、発行済みか否かの判定をする。

その結果、発行済みのICカードであると判定されたときには、演算処理部3に外部装置から送信されたデータブロックを渡す。演算処理部3は、ステップ④aにおいてデータブロックのコマンド部分をデコードして、コマンドに対する処理を実行する。そして、ステップ⑤aで処理した結果の応答情報を外部装置に送出してステップ①の初期状態に戻る。

一方、先のステップ④aの判定で発行済みでないと判定されたときには、ステップ④bでエラー処理として命令エラーのレスポンス（応答）を外部装置へ送出してステップ①の初期状態に戻る。

このような発行処理が終了すると、ICカード10は、その後、外部装置から排出されることになる。外部装置からICカード10が排出される



とICカード10がバックアップ電源を持っていないので、そのRAM4のデータは、すべて消去される。そこで、前記の発行処理プログラムをRAM4に割り当てられたアドレス空間に格納すれば、先のステップ④の発行処理プログラムの消去処理を省略することができる。すなわち、発行処理プログラムをRAM4に記憶するようにした場合には、ICカード10の排出と同時に発行処理プログラムがそのとき消去される。

このようにして発行処理プログラムを発行処理終了とともに消去することにより、カード発行者等によるICカード発行処理時のみ、ICカード内に発行処理プログラムが存在していて、それ以外では存在しないことになり、ICカード使用時或いは運用時に、ICカード内に残っている発行処理プログラムを利用してのデータの読出し、書き込みなどの不正使用を防止することができる。

なお、EEPROM5又はRAM4における消去された発行処理の記憶エリアは、発行処理後の使用時或いは運用時には、動作プログラムのワー

クエリア等として利用される。

ところで、この実施例の場合、識別手段2、演算処理部3、発行処理プログラム書き込み手段8、発行処理プログラム実行手段7、そして発行処理プログラム消去手段8のそれぞれの構成要素の一部或いは全部をEEPROM5ではなく、RAM4にプログラムとして格納するような場合には、前記処理に先立って、ROM3aの処理プログラムに従ってRAM4にこれら機能に対応するプログラムが格納されることになる。

以上説明してきたが、実施例では、揮発性メモリとしてRAMを用いているが、揮発可能なEEPROMを用いてもよいことはもちろんである。また、EEPROMに書き込まれた発行処理プログラムの消去は、外部装置からの指令により発行処理プログラム消去手段を起動して消去するようにしてもよい。また、発行処理プログラムの実行についても、その書き込みとは切離して外部装置からの指令に応じて行われてもよい。

実施例では、識別手段2、演算処理部3、発行

処理プログラム書き込み手段8、発行処理プログラム実行手段7、そして発行処理プログラム消去手段8を独立の手段として説明しているが、これらは、演算処理部3がそれぞれに対応する処理プログラムを実行することで実現されてもよい。

また、実施例では、データブロックにモード識別情報をおき、モード識別手段により発行処理プログラムの格納可否かの識別をしているが、これは、単に、伝送された情報からそれを検出できる手段であればよく、モード識別を行う手段によることに限定されるものではない。

実施例では、データブロックにコマンドとデータとを挿入して伝送している形式のものを挙げているが、これは、コマンドとデータとが独立に伝送されるものであってもよい。

#### 【発明の効果】

以上説明したように、この発明では、外部装置から送付される情報に対して検出手段によってICカードの発行処理プログラムについてのものか否かを検出し、それが検出されると、発行処理プ

ログラムの情報が発行処理プログラム書き込み手段により揮発性メモリ若しくは揮発させることが可能なメモリ内へ書き込まれる。そして、書き込み終了後にそのプログラムがプログラム実行手段により実行されるので、発行者対応に自由にICカードの発行処理を行うことができ、かつ発行処理後には、データを揮発させることが可能なメモリでは、発行処理プログラムに関するデータが、例えば、プログラム実行手段により消去され、揮発性メモリでは、ICカードが外部装置から排出されるときに発行処理プログラムが消去される。

その結果、ICカードの使用時或いは運用時には、ICカード内部に発行処理プログラムを残さなくても済み、揮発性メモリの空間若しくはデータを揮発させることが可能なメモリの空間は、動作プログラムのワークエリア等として利用できるようになり、メモリ領域を十分に活用でき、かつ機密性、信頼性に優れたICカードを発行することができる。

#### 4.図面の簡単な説明

代理人 弁理士 梶 山 侑 是  
弁理士 山 本 富士男

```

graph TD
    Start([開始]) --> J1{データ受信? ①}
    J1 -- No --> J1
    J1 -- Yes --> J2{実行処理? ②}
    J2 -- No --> J3{実行済? ③a}
    J2 -- Yes --> J3
    J3 -- No --> J4{命令エラー・リボンス  
を外部へ送信 ④}
    J3 -- Yes --> J5{コマンドに対する  
処理実行 ④a}
    J5 --> J6{実行実行結果  
を外部へ送信 ⑤a}
    J6 --> J7{実行処理プログラムを消去 ⑧}
    J7 --> J8{実行フラグを  
実行済にセット ⑨}
    J8 --> J1
    J4 --> J1
    
```

Figure 1 is a flowchart illustrating the program execution process. The process begins with a start terminal (開始). It then enters a loop starting with a decision diamond (1) "データ受信?" (Data received?). If the answer is "No", it loops back to the start. If "Yes", it proceeds to decision diamond (2) "実行処理?" (Execute processing?). If the answer is "No", it proceeds to decision diamond (3a) "実行済?" (Execution completed?). If the answer is "Yes", it proceeds to decision diamond (3a). If the answer to (3a) is "No", it proceeds to process block (4) "命令エラー・リボンスを外部へ送信" (Send command error/reboot to external). If the answer to (3a) is "Yes", it proceeds to process block (4a) "コマンドに対する処理実行" (Execute processing for command). From (4a), it proceeds to process block (5a) "実行実行結果を外部へ送信" (Send execution execution result to external). From (5a), it proceeds to process block (8) "実行処理プログラムを消去" (Delete execution processing program). From (8), it proceeds to process block (9) "実行フラグを執行済にセット" (Set execution flag to execution completed). From (9), it loops back to the start of the loop (1). From process block (4), it also loops back to the start of the loop (1).